EXHIBIT 1

AFFIDAVIT IN SUPPORT OF A SEARCH WARRANT APPLICATION

I, David J. Pawson, being first duly sworn, hereby state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the premises known as 38 David Drive, York, Maine, hereinafter "PREMISES," further described in Attachment A, for the things described in Attachment B.

2. I have been employed as a Special Agent ("SA") of U.S. Department of Homeland Security, Homeland Security Investigations ("HSI"), since 2009, and am currently assigned to Portland, Maine. While employed by HSI, I have investigated federal criminal violations related to high technology or cybercrime, child exploitation, and child pornography. I have gained experience through training at the Federal Law Enforcement Training Center located in Brunswick, Georgia and my work often relates to conducting these types of investigations. I have received training in the area of child pornography and child exploitation and have had the opportunity to observe and review numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in all forms of media including computer media.

3. Moreover, I am a federal law enforcement officer who is engaged in enforcing the criminal laws, including 18 U.S.C. §§ 2251, 2252, and 2252A, and I am authorized by law to request a search warrant.

4. The statements contained in this affidavit are based in part on information provided by U.S. federal law enforcement agents; written reports about this and other investigations that I have received, directly or indirectly, from other law enforcement agents,

including foreign law enforcement agencies; information gathered from the service of administrative subpoenas; the results of physical and electronic surveillance conducted by law enforcement agents; independent investigation and analysis by law enforcement agents/analysts and computer forensic professionals; and my experience, training and background as a Special Agent. Since this Affidavit is being submitted for the limited purpose of securing a search warrant, I have set forth only the facts that I believe are necessary to establish probable cause to believe that contraband and evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 2252A(a)(1) (transportation of child pornography) and 2252A(a)(5)(B) (possession of and access with intent to view child pornography) are presently located at the PREMISES.

PROBABLE CAUSE

5. A user of the internet account at the PREMISES has uploaded to cloud storage 903 images or videos depicting minors engaging in sexually explicit conduct including sexual intercourse between minors and between minors and adults. The images and videos prompted Dropbox Inc. to report the incident to the National Center for Missing and Exploited Children (NCMEC). There is probable cause to believe that a user of the internet account at the PREMISES accessed the Dropbox account to upload and store digital files depicting minors engaging in sexually explicit conduct, as further described herein.

6. Dropbox is an internet hosting service specifically designed to host user files. It allows users to upload files that can be remotely accessed over the internet after a username and password or another authentication is provided without having to store files on the user's computer. Typically, the services allow a user to browse and preview files from any of the user's

linked devices provided the user has the appropriate user credentials and password. Related services are content-displaying hosting services, virtual storage and remote backup.

7. On May 15, 2020, my office received NCMEC Cyber Tipline Report 70855404. The report was initially sent to HSI's Cyber Crimes Center, which then forwarded it to HSI Portland. The report was based on information provided to NCMEC by Dropbox on April 25, 2020. Dropbox reported that a Dropbox user had uploaded approximately 903 sexually explicit images and videos of minors to the user's Dropbox account. Dropbox identified the user's email address as jpease1020@gmail.com, with a screen/user name of Jackson Patrick and a User ID number of 680892311. Dropbox also provided information indicating that the user had logged into the account on three occasions in April 2020 using the IP address 98.11.110.46, including April 25, 2020, at 01:14:36 GMT.

8. Dropbox also provided NCMEC with copies of the 903 files that the user of the jpease1020@gmail.com account had uploaded. On May 18, 2020, I reviewed those files, including the following:

a. _OG4IB6DK.jpg: This image depicts a minor male, approximately 10 years old, lying on his back, nude with his hands and feet tied with a blue cloth. The boy is being anally penetrated by an adult penis. A copy of the image is attached under seal as Exhibit 1.

b. 001m-003-20150217-231631477.jpg: This image depicts a minor male, approximately six months to two years old, positioned on his back wearing a green "onesie" which has been unbutton an pulled up to the waistline exposing his penis. An adult male penis is also depicted and appears to be resting on the child's anus.

c. 00-350.jpg: This image depicts a male, approximately nine to 12 years old, lying on his right side wearing a dark colored shirt and is nude from the waist down. An adult pair of hands is also depicted, one pressing on the left buttocks of the boy and the second hand is inserting a middle finger into the boy's anus.

9. During my review, I noticed many of these files' names indicate they were obtained via the social media application Kik. Individuals interested in exchanging child exploitation material have been using Kik for this purpose for several years. The application grants users anonymity and allows them to send and receive images that are not stored on phones. The application is also gaining a reputation for predators who anonymously seek out children for inappropriate and obscene activity such as enticing the creation of child exploitation material.

10. On June 2, 2020, Google identified the subscriber of email account jpease1020@gmail.com as Joshua Pease, associated with Google Account ID 684964516710. Google also identified an associated email account assigned Google Account ID 971475312966 in the name of Jack Pats with assigned email address 1020gaygay@gmail.com. The email address jpease1020@gmail.com is the recovery email for this account.

11. Google also provided timestamped IP address activity for the aforementioned Gmail accounts for the period April 23, 2020, through May 26, 2020. In each instance, these email accounts were accessed from IP address 98.11.110.46, the same IP address from which the explicit digital files were uploaded to the suspect Dropbox account.

12. According to publicly available information, IP address 98.11.110.46, which was used to access Dropbox on April 25, 2020, at 1:14:00 a.m. GMT, was registered to Charter Communications, Inc.

13. On May 15, 2020, a subpoena was issued to Charter Communications, Inc., seeking information on the Charter subscriber assigned IP address 98.11.110.46 at the relevant time. Charter responded to the subpoena on May 22, 2020, and provided the following information on the subscriber:

Subscriber Name: Donald Pease

Phone: 207-363-1588

Subscriber Address: 38 David Drive, York, Maine 03909

Account Number: 725185601

Account Status: Active

14. On June 10, 2020, HSI Special Agent James Bell met with York, Maine Police and learned that a Joshua Pease with a year of birth of 2001 resides at the PREMISES. Police records indicate that the York police encountered Joshua Pease for an unrelated issue. Joshua Pease was driving a 2001 Subaru Legacy with Maine license 5974UM, registered to Donald Pease at the PREMISES.

15. A check of the Maine Bureau of Motor Vehicles databases on about June 15, 2020, revealed that an individual named Joshua Pease with a date of birth in October 2001 was issued a Maine driver's license listing the address of the PREMISES.

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

16. As described above and in Attachment B, this application seeks permission to search for records that might be found on the PREMISES, in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

17. *Probable cause.* I submit that if a computer or storage medium is found on the PREMISES, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the internet are sometimes automatically downloaded into a temporary internet directory or "cache."

18. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the PREMISES because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the

attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer owner.

c. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological

context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

d. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

e. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and

passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

f. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

g. I know that when an individual uses a computer to upload child pornography, the individual's computer will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The computer is an instrumentality of the crime because it is used as a means of committing the criminal offense. The computer is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that a computer used to commit a crime of this type may contain: data that is evidence of how the computer was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of internet discussions about the crime; and other records that indicate the nature of the offense.

19. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete

electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the PREMISES. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

20. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

21. Because several people share the PREMISES as a residence, it is possible that the PREMISES will contain storage media that are predominantly used, and perhaps owned, by persons who are not suspected of a crime. If it is nonetheless determined that that it is possible that the things described in this warrant could be found on any of those computers or storage media, the warrant applied for would permit the seizure and review of those items as well.

CONCLUSION

22. I submit that this affidavit supports probable cause for a warrant to search the PREMISES described in Attachment A and seize the items described in Attachment B.

Respectfully submitted,

David J. Pawson
Special Agent
Homeland Security Investigations

Sworn to telephonically and signed electronically in accordance with the requirements of Fed. R. Crim. P. 4.1 on August 4, 2020:

Sworn to telephonically and signed electronically in accordance with the requirements of Fed. R. Crim P. 4.1

Date and Time:
August 4, 2020, 12:36 p.m.

City and State:
Portland, ME

John H. Rich III,
U.S. Magistrate Judge